



**UNITED STATES DEPARTMENT OF COMMERCE**  
**National Institute of Standards and Technology**  
Gaithersburg, Maryland 20899-0001

SEP 23 2019

Mr. Steve Weis  
MuckRock News  
DEPT MR 78756  
411A Highland Ave  
Somerville, MA 02144-2516

Dear Mr. Weis,

This letter serves as the final response to your August 9, 2019 Freedom of Information Act (FOIA) request (FOIA Log #DOC-NIST-2019-001948) to the National Institute of Standards and Technology (NIST) for:

Any documents related to the choice of elliptic curves over prime fields for ECC key agreement that first appeared in FIPS 186-4 Appendix D, sections D.1.2.1-D.1.2.5 (<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>). For example, any information to the choice of D.1.2.3: P-256: SEED = c49d3608 86e70493 6a6678e1 139d26b7 819f7e90.

This document has been superseded by NIST 800-56A (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf>). Please return any email, memorandum, presentations, reports, articles, research papers, justifying the choice of initialization parameters for the following standards: P-224 (also known as secp224r1), P-256 (secp256r1), P-384 (secp384r1), P-521 (secp521r1) Dr. Jerry (or Gerald) Solinas from the NSA may have been involved in the parameter selection.

NIST has no documents that are responsive to your request. If you have questions or concerns or would like to discuss any aspect of your request, you may contact either the analyst who processed your request, Maureen O'Reilly by telephone at 301-975-3189, or by email at [maureen.oreilly@nist.gov](mailto:maureen.oreilly@nist.gov) or me, the FOIA Public Liaison/Freedom of Information Act Officer, at 301-975-4054. We may also be reached at [foia@nist.gov](mailto:foia@nist.gov).

Please refer to your FOIA request tracking number, DOC-NIST-2019-001948, when contacting us.

In addition, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

**NIST**

Office of Government Information Services  
National Archives and Records Administration  
8601 Adelphi Road-OGIS  
College Park, Maryland 20740-6001  
e-mail at [ogis@nara.gov](mailto:ogis@nara.gov)  
telephone at 202-741-5770; toll free at 1-877-684-6448, or facsimile at 202-741-5769

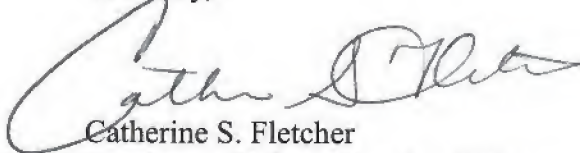
You have the right to appeal this response to your FOIA request. An appeal must be received within 90 calendar days of the date of this response letter. Address your appeal to the following office:

Assistant General Counsel for Employment, Litigation and Information  
U.S. Department of Commerce  
Office of the General Counsel, Room 5896  
1401 Constitution Ave., NW  
Washington, D.C. 20230

An appeal may also be sent by e-mail to [FOIAAppeals@doc.gov](mailto:FOIAAppeals@doc.gov), or by FOIAonline, if you have an account in FOIAonline, at <https://foiaonline.regulations.gov/foia/action/public/home#>. The appeal should include a copy of the original request and an initial denial, if any. All appeals should include a statement of the reasons why the records requested should be made available and why the adverse determination was in error.

The appeal letter, the envelope, and the e-mail subject line should be clearly marked "Freedom of Information Act Appeal." The e-mail, FOIAonline and office are monitored only on working days during normal business hours (8:30 a.m. to 5:00 p.m., Eastern Time, Monday through Friday). FOIA appeals posted to the e-mail box, FOIAonline, or office after normal business hours will be deemed received on the next normal business day. If the 90<sup>th</sup> calendar day for submitting an appeal falls on a Saturday, Sunday or legal public holiday, an appeal received by 5:00 p.m., Eastern Standard Time, the next business day will be deemed timely.

Sincerely,

A handwritten signature in dark ink, appearing to read "Catherine S. Fletcher", is written over a horizontal line.

Catherine S. Fletcher  
Freedom of Information Act Officer